UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/564,986	01/18/2006	Satoshi Niwano	2005_1909A	7145

52349 7590 12/24/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
RAAB, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2169	

MAIL DATE	DELIVERY MODE
12/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/564,986	NIWANO ET AL.	
	Examiner	Art Unit	
	Christopher J. Raab	2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-84* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-84* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/18/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Preliminary Amendment

01. The present Office Action is based upon the original patent application filed on 01/18/06 as modified by the preliminary amendment files on 01/18/06 filed. **Claims 47 – 84** are now pending in the present application.

Information Disclosure Statement

02. The information disclosure statement (IDS) filed on **01/18/08** has been considered by the examiner and made of record in the application file.

Priority

03. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

04. The drawings were received on **01/18/06**. These drawings are accepted.

Claim Rejections - 35 USC § 101

05. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

06. **Claims 47 – 80** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims lack a useful, concrete, and tangible result within the meaning of 35 USC 101.

The tangible requirement does not necessarily mean that a claim must either be tied to a particular machine or apparatus, or must operate to change articles or materials to a different state or thing. However, the tangible requirement does require that the claim must recite more than a 101 judicial exception, in that the process claim must set forth a practical application of that 101 judicial exception to produce a real-world result. Providing a benefit to the recipient if the recipient has performed the activity does not produce a real-world result and is clearly just an abstract idea. Therefore the claims do not provide a tangible result.

In view of the above analysis, applicant's claims are processes, which include a judicial exception therein. Upon review of the claims as a whole, there is no transformation nor do the claims produce a useful, concrete, and tangible result. Accordingly, the claims are non-statutory under 35 U.S.C. 101.

07. **Claims 47 – 80** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed towards a method of judging use permission. According to MPEP § 2106.IV.B, the first step in determining whether a claim recites patent eligible subject matter is to determine whether the claim falls within one of the four statutory categories of invention recited in 35 U.S.C. 101: process, machine, manufacture and composition of matter. The latter three categories

define "things" or "products," while a "process" consists of a series of steps or acts to be performed. For purposes of §101, a "process" has been given a specialized, limited meaning in the courts. Based on a Supreme Court precedent and recent Federal Circuit decisions, a claimed process is patent-eligible under §101 if: (1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing." Since the claim fails to meet the requirements mentioned above to place the claim in the statutory category of a process, the claim fails to fall within one of the four statutory categories (i.e., process, machine, manufacture, or composition of matter).

08. **Claims 81 – 84** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, function descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are nonstatutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive

material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

Claim Rejections - 35 USC § 102

09. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office Action:

A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. **Claims 47 – 59, and 69 – 84** are rejected under 35 U.S.C. 102(e) as being unpatentable over **Muntz et al. (US PGPub 2003/0208681)**, hereinafter 'Muntz'.

Consider **claim 47**, Muntz discloses a method of judging use permission of information used by one or more terminal apparatuses which use content provided by a content provided and metadata which is data provided by a metadata provider and supplementing the content (paragraphs [0002] – [0004]), comprising:

locating metadata from a server upon accessing a file (read as judging use permission of the metadata based on usage control information regarding use control of the metadata) (paragraph [0015]);

the metadata containing the file and file system attributes (read as using the metadata in the case where it is judged that the use of the metadata is permitted in said judging) (paragraph [0015]);

such that different users can have different access privileges (read as wherein the usage control information includes first signer identification information identifying a range of a provider of metadata that can be used) (paragraph [0016]);

the metadata containing a list of credentials for the users (read as a signature of the metadata provider is included in the metadata) (paragraph [0016]);

a validation mechanism, which can contain include a token, comprising credentials, such as privilege and authority signature (read as second signer identification information is included in a public key certificate used for verifying the signature of the metadata, the second signer identification information identifying at least one of the signer of the metadata and the signer of the public key certificate) (paragraphs [0019], [0023]);

the metadata being used when a request is made by the user, such that a token be generated which allows the user to perform certain operations (read as in said judging, it is judged whether the metadata use is permitted based on the metadata provider identified in the first signer identification information, the second signer

identification, and the signature verification using the public key certificate) (paragraph [0023]);

the token created being specific for the user (read as the first signer identification information includes information identifying the signer of the metadata) (paragraphs [0023] – [0024]).

Consider **claim 48**, and **as applied to claim 47 above**, Muntz discloses a method such that a certificate or ticket is used for a user to authenticate to the system (read as wherein the one or more terminal apparatuses hold the public key certificate used for the signature verification of the metadata signer, and in said judging, it is judged that the use of the metadata is permitted in the case where (i) the signature verification of the metadata is successful using the public key certificate held by the one or more terminal apparatuses, and (ii) the subject of the public key certificate corresponds with the identification of the first signer identification information) (paragraph [0032]).

Consider **claim 49**, and **as applied to claim 47 above**, Muntz discloses a method such that multiple users can authenticate to the system, based on user credential data (read as wherein the one or more terminal apparatuses previously hold third signer identification information uniquely identifying the second signer identification information, and in said judging, it is judged that the use of the metadata is permitted in the case where the third signer identification information corresponds with the second signer identification information) (paragraphs [0016], [0031]).

Consider **claim 50**, and **as applied to claim 47 above**, Muntz discloses a method such that multiple user account information is stored at the metadata server (read as the content includes third signer identification information uniquely identifying the second signer identification information, and in said judging, it is judged that the use of the metadata is permitted in the case where the third signer identification information corresponds with the second signer identification information) (paragraphs [0016], [0031]).

Consider **claim 51**, and **as applied to claim 47 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user (read as the metadata is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the metadata, and hold a second license for using the metadata, third signer identification information is included in the second license, the third signer identification information uniquely identifying the second signer identification information, and in said judging, the use of the metadata is permitted in the case where third signer identification information corresponds with the second signer identification information, the third signer identification information uniquely identifying the second signer identification information included in the second license) (paragraphs [0016], [0024]).

Consider **claim 52**, and **as applied to claim 47 above**, Muntz discloses a method such that the metadata can uniquely identifier each user (read as the first signer identification information includes third signer identification information uniquely identifying the second signer identification information) (paragraphs [0016], [0023]).

Consider **claim 53**, and **as applied to claim 47 above**, Muntz discloses a method of generating metadata, but does not specifically disclose that metadata is generated by the user.

In the same field of endeavor, Lowe discloses a method such that the user can create and manage the metadata (read as user identification information is included in user metadata generated by a user in the one or more terminal apparatuses) (paragraphs [0017], [0069]).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the metadata management taught by Lowe into the user identification method taught for the purpose of allowing users to have control over the metadata.

Consider **claim 54**, and **as applied to claim 53 above**, Muntz discloses a method such that the user can be given full permission (read as for the user metadata, a digital signature is omitted, and in said judging, verification of the signature is omitted) (paragraph [0023]).

Consider **claim 55**, and **as applied to claim 53 above**, Muntz discloses a method such that the metadata is encrypted (read as the user metadata is at least partially encrypted) (paragraph [0024]).

Consider **claim 56**, and **as applied to claim 55 above**, Muntz discloses a method such that the user device holds a secret key to aid in decryption of the information (read as the one or more terminal apparatuses hold secret information

common to the one or more terminal apparatuses owned by the user, and the secret information decrypts the user metadata) (paragraphs [0021], [0026]).

Consider **claim 57**, and **as applied to claim 47 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the content is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the content, and hold a first license for using the content, and a first signed identification information is included in the first license) (paragraphs [0016], [0024], [0026]).

Consider **claim 58**, and **as applied to claim 47 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the content is encrypted, and the first signer identification information is included in the encrypted content) (paragraphs [0016], [0024], [0026]).

Consider **claim 59**, and **as applied to claim 47 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the first signed identification information includes an encryption key for decrypting the encrypted metadata, and is included in a second license for using the metadata) (paragraphs [0016], [0024], [0026]).

Consider **claim 69**, and **as applied to claim 47 above**, Muntz discloses a method such that metadata controls which permission the user has (read as the usage control information includes control permission information indicating use permission of

user metadata generated by a user in the one or more terminal apparatuses, and in said judging, metadata use permission is judged based on the control permission information) (paragraphs [0016], [0023]).

Consider **claim 70**, and **as applied to claim 69 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the content is encrypted,

the one or more terminal apparatuses include an encryption key for decrypting the content, and hold a first license for using the content, and the revision permission information is included in the first license) (paragraphs [0016], [0024], [0026]).

Consider **claim 71**, and **as applied to claim 69 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read the content is encrypted,

the one or more terminal apparatuses include an encryption key for decrypting the content, and hold a first license for using the content, and the revision permission information is included in the content) (paragraphs [0016], [0024], [0026]).

Consider **claim 72**, and **as applied to claim 47 above**, Muntz discloses a method such that the metadata controls which user are given which permission, such that the information to be related to a user or a device used by a user (read as the usage control information includes moving range specifying information which specifies moving range of user metadata generated by a user in the one or more terminal apparatuses, and in said judging, metadata use permission is judged based on the moving range specifying information) (paragraphs [0016], [0024], [0026]).

Consider **claim 73**, and **as applied to claim 47 above**, Muntz discloses a method such that the metadata controls which user are given which permission, such that the information to be related to a user or a device used by a user (read as the case where the moving range specifying information indicates unlimited moving range, the metadata includes user identification information indicating that the metadata is user metadata generated in the one or more terminal apparatuses by a user, for the user metadata a digital signature is omitted, and in said judging, in the case where the user identification information is included, verification of the signature is omitted) (paragraphs [0016], [0024], [0026]).

Consider **claim 74**, and **as applied to claim 72 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as at least a part of the user metadata generated by the user in the one or more terminal apparatuses is encrypted using an encryption key common to the one or more terminal apparatuses owned by the user, and in said metadata use permission judging, in the case where the moving range specifying information indicates that the moving range is limited to the one or more terminal apparatuses owned by the user, it is judged that the use of the user metadata is permitted in one or more terminal apparatuses which can decrypt the user metadata) (paragraphs [0016], [0024], [0026]).

Consider **claim 75**, and **as applied to claim 74 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the encryption key

common to the one or more terminal apparatuses is secret information common to the one or more terminal apparatuses owned by the user, and for the user metadata, at least a part of the user metadata is encrypted using the secret information) (paragraphs [0016], [0024], [0026]).

Consider **claim 76**, and **as applied to claim 72 above**, Muntz discloses a method such that users are given a certain permission based on access privileges (read as the user metadata is assigned with a digital signature of the one or more terminal apparatuses which have generated the user metadata, and in said metadata use permission judging, the one or more terminal apparatuses which have generated the user metadata are identified) (paragraphs [0016], [0024]).

Consider **claim 77**, and **as applied to claim 72 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the content is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the content, and hold a first license for using the content, and the revision permission information is included in the first license) (paragraphs [0016], [0024], [0026]).

Consider **claim 78**, and **as applied to claim 72 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read the content is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the content, and hold a first license for using the content, and the revision permission information is included in the content) (paragraphs [0016], [0024], [0026]).

Consider **claim 79**, and **as applied to claim 72 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the metadata is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the metadata, and hold a second license for using the metadata, and the revision permission information is included in the second license) (paragraphs [0016], [0024], [0026]).

Consider **claim 80**, and **as applied to claim 72 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read the metadata is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the metadata, and hold a second license for using the metadata, and the revision permission information is included in the metadata) (paragraphs [0016], [0024], [0026]).

Consider **claim 81**, Muntz discloses one or more terminal apparatuses which use content provided by a content provider and metadata which is data provided by a metadata provided and supplementing the content (paragraphs [0002] – [0004]), comprising:

locating metadata from a server upon accessing a file (read as metadata user permission judging unit operable to judge user permission of the metadata based on usage control information regarding use control of the metadata) (paragraph [0015]);

the metadata containing the file and file system attributes (read as use unit operable to use the metadata in the case where it is judged that the use of the metadata is permitted in said judging) (paragraph [0015]);

such that different users can have different access privileges (read as the usage control information includes first signer identification information identifying a range of a provider of metadata that can be used) (paragraph [0016]);

the metadata containing a list of credentials for the users (read as a signature of the metadata provider is included in the metadata) (paragraph [0016]);

a validation mechanism, which can contain include a token, comprising credentials, such as privilege and authority signature (read as second signer identification information is included in a public key certificate used for verifying the signature of the metadata, the second signer identification information identifying at least one of the signer of the metadata and the signer of the public key certificate) (paragraphs [0019], [0023]);

the metadata being used when a request is made by the user, such that a token be generated which allows the user to perform certain operations (read as in said judging, it is judged whether the metadata use is permitted based on the metadata provider identified in the first signer identification information, the second signer identification, and the signature verification using the public key certificate) (paragraph [0023]);

the token created being specific for the user (read as the first signer identification information includes information identifying the signer of the metadata) (paragraphs [0023] – [0024]).

Consider **claim 82**, Muntz discloses a transmitting apparatus which transmits, to one or more terminal apparatuses, content provided by a content provider and metadata which is data, provided by a metadata provider, supplementing the content, based on a request, the apparatus (paragraphs [0002] – [0004]), comprising:

locating metadata from a server upon accessing a file (read as a means to transmit usage control information regarding use control of the metadata so as to have the one or more terminal apparatuses judge use permission of the metadata) (paragraph [0015]);

such that different users can have different access privileges (read as wherein the usage control information includes first signer identification information identifying a range of a provider of metadata that can be used) (paragraph [0016]);

the metadata containing a list of credentials for the users (read as a signature of the metadata provider is included in the metadata) (paragraph [0016]);

a validation mechanism, which can contain include a token, comprising credentials, such as privilege and authority signature (read as second signer identification information is included in a public key certificate used for verifying the signature of the metadata, the second signer identification information identifying at least one of the signer of the metadata and the signer of the public key certificate) (paragraphs [0019], [0023]);

the metadata being used when a request is made by the user, such that a token be generated which allows the user to perform certain operations (read as in said judging, it is judged whether the metadata use is permitted based on the metadata provider identified in the first signer identification information, the second signer identification, and the signature verification using the public key certificate) (paragraph [0023]);

the token created being specific for the user (read as the first signer identification information includes information identifying the signer of the metadata) (paragraphs [0023] – [0024]).

Consider **claim 83**, Muntz discloses a content distribution system, comprising the one or more terminal apparatuses according to claim 81 and a transmitting apparatus which transmits, to the one or more terminal apparatuses, content provided by a content provider and metadata which is data, provided by a metadata provider, supplementing the content, based on a request (paragraphs [0002] – [0004]), comprising:

locating metadata from a server upon accessing a file (read as judging use permission of the metadata based on usage control information regarding use control of the metadata) (paragraph [0015]);

the metadata containing the file and file system attributes (read as a means to transmit usage control information regarding use control of the metadata so as to have the one or more terminal apparatuses judge use permission of the metadata) (paragraph [0015]);

such that different users can have different access privileges (read as wherein the usage control information includes first signer identification information identifying a range of a provider of metadata that can be used) (paragraph [0016]);

the metadata containing a list of credentials for the users (read as a signature of the metadata provider is included in the metadata) (paragraph [0016]);

a validation mechanism, which can contain include a token, comprising credentials, such as privilege and authority signature (read as second signer identification information is included in a public key certificate used for verifying the signature of the metadata, the second signer identification information identifying at least one of the signer of the metadata and the signer of the public key certificate) (paragraphs [0019], [0023]);

the metadata being used when a request is made by the user, such that a token be generated which allows the user to perform certain operations (read as in said judging, it is judged whether the metadata use is permitted based on the metadata provider identified in the first signer identification information, the second signer identification, and the signature verification using the public key certificate) (paragraph [0023]);

the token created being specific for the user (read as the first signer identification information includes information identifying the signer of the metadata) (paragraphs [0023] – [0024]).

Consider **claim 84**, Muntz discloses program for judging use permission of information used by one or more terminal apparatuses which use content provided by a

content provided and metadata which is data provided by a metadata provider and supplementing the content (paragraphs [0002] – [0004]), comprising:

locating metadata from a server upon accessing a file (read as judging use permission of the metadata based on usage control information regarding use control of the metadata) (paragraph [0015]);

the metadata containing the file and file system attributes (read as using the metadata in the case where it is judged that the use of the metadata is permitted in said judging) (paragraph [0015]);

such that different users can have different access privileges (read as wherein the usage control information includes first signer identification information identifying a range of a provider of metadata that can be used) (paragraph [0016]);

the metadata containing a list of credentials for the users (read as a signature of the metadata provider is included in the metadata) (paragraph [0016]);

a validation mechanism, which can contain include a token, comprising credentials, such as privilege and authority signature (read as second signer identification information is included in a public key certificate used for verifying the signature of the metadata, the second signer identification information identifying at least one of the signer of the metadata and the signer of the public key certificate) (paragraphs [0019], [0023]);

the metadata being used when a request is made by the user, such that a token be generated which allows the user to perform certain operations (read as in said judging, it is judged whether the metadata use is permitted based on the metadata

provider identified in the first signer identification information, the second signer identification, and the signature verification using the public key certificate) (paragraph [0023]);

the token created being specific for the user (read as the first signer identification information includes information identifying the signer of the metadata) (paragraphs [0023] – [0024]).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. **Claims 60 – 68** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Muntz et al. (US PGPub 2003/0208681)**, hereinafter 'Muntz' in view of **Lowe et al. (US PGPub 2004/0267693)**, hereinafter 'Lowe'.

Consider **claim 60**, and **as applied to claim 47 above**, Muntz discloses a method for utilizing information, however Muntz does not specifically disclose that a user can create and modify the metadata.

In the same field of endeavor, Lowe discloses a method such that a user can have control over the metadata, by allowing the user to create, modify, and manage the metadata (read as the usage control information includes revision permission information indicating revision permission of metadata, said method for judging user permission of information further includes judging revision permission of metadata based on the revision permission information) (paragraphs [0017], [0069]).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the metadata management taught by Lowe into the user identification method taught for the purpose of allowing users to have control over the metadata.

Consider **claim 61**, and **as applied to claim 60 above**, Lowe discloses a method such that the user can be given permission to modify the metadata (read as the revision permission information is information identifying whether revision can be permitted or not) (paragraphs [0017], [0069]).

Consider **claim 62**, and **as applied to claim 60 above**, Lowe discloses a method such that user can modify the metadata (read as the revision permission information is identification information which uniquely identifies the metadata) (paragraphs [0017], [0069]).

Consider **claim 63**, and **as applied to claim 61 above**, Lowe discloses a method such that a user can be assigned the right to access and modify the metadata (read as the revision permission information is identification information which identifies the provider of the metadata which can be revised, using the first signer identification information) (paragraphs [0017], [0069]).

Consider **claim 64**, and **as applied to claim 60 above**, Lowe discloses a method such that each user can be given the permission to modify data (read as the usage control information includes revision permission information indicating revision permission of metadata, and said method for judging use permission of information further includes judging revision permission of metadata based on the revision permission information) (paragraphs [0017], [0069]).

Consider **claim 65**, and **as applied to claim 60 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the content is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the content, and hold a first license for using the content, and the revision permission information is included in the first license) (paragraphs [0016], [0024], [0026]).

Consider **claim 66**, and **as applied to claim 60 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read the content is encrypted,

the one or more terminal apparatuses include an encryption key for decrypting the content, and hold a first license for using the content, and the revision permission information is included in the content) (paragraphs [0016], [0024], [0026]).

Consider **claim 67**, and **as applied to claim 60 above**, Muntz discloses a method such that the metadata is encrypted in order to create an encrypted token for the user, and decrypting the information using a key (read as the metadata is encrypted, the one or more terminal apparatuses include an encryption key for decrypting the metadata, and hold a second license for using the metadata, and the revision permission information is included in the second license) (paragraphs [0016], [0024], [0026]).

Consider **claim 68**, and **as applied to claim 60 above**, Lowe discloses a method such that each user permission to modify the metadata can be stored in the metadata (read as the revision permission information is included in the metadata) (paragraphs [0017], [0069]).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) Brock, Anthony Paul et al.	US PGPub	2008/0021926
b) Saari, Timo et al.	US Patent	7,216,131
c) Apparao, Vidur et al.	US Patent	7,213,036
d) Apparao V et al.	US PGPub	2005/0038813

e) Gustman, Samuel US Patent 6,353,831

15. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

16. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Christopher Raab whose telephone number is (571) 270-1090. The Examiner can normally be reached on Monday-Friday from 8:30am to 6:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Pierre Vital can be reached on (571) 272-4215. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Christopher Raab
C.R./cr

December 19, 2008

/Pierre M. Vital/
Supervisory Patent Examiner, Art Unit 2169